

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-267957

(43)Date of publication of application : 29.09.2000

(51)Int. Cl. G06F 13/00

G06F 9/46

H04L 12/46

H04L 12/28

(21)Application number : 11-069575

(71)Applicant : HITACHI LTD

(22)Date of filing : 16.03.1999

(72)Inventor : FURUYA MASATOSHI

SEKOZAWA TERUJI

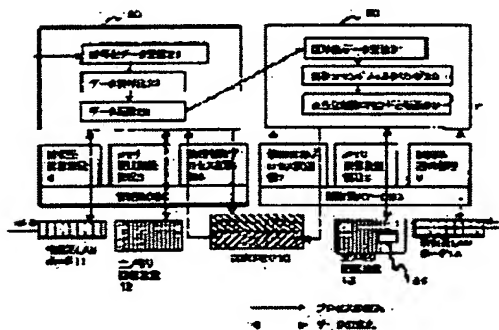
KATO HIROMITSU

(54) FIRE WALL FOR CONTROL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain the fire wall which has a function of transferring only commands useful to the control system to the control system by filtering commands obtained by inter-process communication and communicating allowed commands to a monitor and control computer.

SOLUTION: The fire wall for control system is mounted on a computer where a general purpose operating system (G-OS) and a dedicated real-time operating system (RT-OS) coexist. Processes on the G-OS and RT-OS are enabled to communicate with each other. At this time, an information system process 20 on the G-OS receives and decodes coded data and passes the decoded data to a control system process 30 on the RT-OS. Then the control system process 30 extracts control commands extracted from the data and transfers only passable commands to a monitor computer, etc., on a control system LAN by referring to a command filtering table.



CU

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-267957

(P2000-267957A)

(43) 公開日 平成12年9月29日 (2000.9.29)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
	9/46		3 6 0 F 5 B 0 9 8
H 0 4 L 12/46	3 6 0	H 0 4 L 11/00	3 1 0 C 5 K 0 3 3
12/28			

審査請求 未請求 請求項の数 5 O L (全 18 頁)

(21) 出願番号 特願平11-69575

(22) 出願日 平成11年3月16日 (1999.3.16)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 古谷 雅年

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 瀬古沢 照治

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100068504

弁理士 小川 勝男

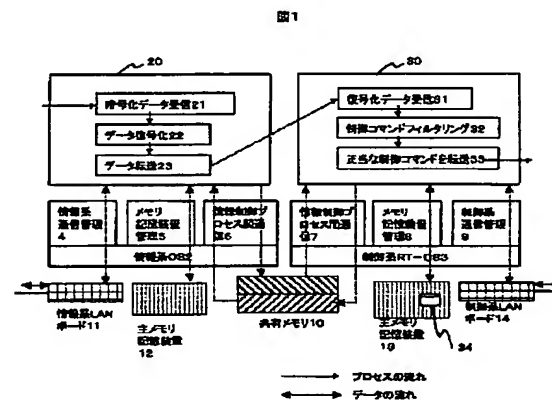
最終頁に続く

(54) 【発明の名称】 制御系用ファイアウォール

(57) 【要約】

【課題】 制御系LANと情報系LANとの接点において、悪意、または、無意識による制御系への不正介入、トラフィック妨害を防ぐための制御系用ファイアウォールを提供する。

【解決手段】 情報系プロセスで、暗号化データを受信し、そのデータを復号化し、復号化したデータを制御系プロセスに渡し、データから制御コマンドを抽出し、コマンドフィルタリングテーブルを参照して、「通過」できる制御コマンドだけフィルタリングして、制御系LAN上の監視制御コンピュータなどに転送する。また、制御系プロセスで、監視データを受信し、プロセス間通信で情報系プロセスに渡し、さらに、情報系LAN上の端末やデータベースサーバに転送する。



【特許請求の範囲】

【請求項1】制御機器を制御したり、計測機器からデータを収集したりする監視制御用コンピュータが接続されている制御系ネットワークに接続する制御系LANボードと、情報端末や情報サーバが接続されている情報系ネットワークに情報系LANボードとを搭載し、制御系用リアルタイムオペレーティングシステムと情報系オペレーティングシステムとが動作し、制御系用通信プロトコルで通信する手段と情報系用通信プロトコルで通信する手段とを有し、制御系用リアルタイムオペレーティングシステム上で動作するプロセスと情報系オペレーティングシステム上で動作するプロセスとがプロセス間通信する手段を有するコンピュータであって、情報系オペレーティングシステム上では、情報系ネットワークから送信された暗号化コマンドを復号化する手段と、復号化したコマンドを制御系用リアルタイムオペレーティングシステム上で動作するプロセスにプロセス間通信する手段とを有し、制御系用リアルタイムオペレーティングシステム上では、プロセス間通信によって入手したコマンドをフィルタリングする手段と、フィルタリング手段によって許可されたコマンドを前記監視制御用コンピュータに通信する手段とを有していることを特徴とする制御系用ファイアウォール。

【請求項2】請求項1記載の制御用ファイアウォールであって、制御系用リアルタイムオペレーティングシステム上では、制御可能なコマンド情報、または、監視データを制御系ネットワークから受信し、受信した内容に基づいてコマンドをフィルタリングするルールを変更する手段を有していることを特徴とする制御系用ファイアウォール。

【請求項3】請求項1記載の制御系用ファイアウォールであって、コマンドフィルタリング手段のためのフィルタリングルールを記憶する記憶装置は、制御系用リアルタイムオペレーティングシステム上で動作するプロセスからのみ読み書き可能なことを特徴とする制御系用ファイアウォール。

【請求項4】請求項1記載の制御系用ファイアウォールであって、情報系オペレーティングシステム上では、コマンドを送信したユーザが正当な権利をもつかを認証する手段と、操作権が登録のものとは一致するかを確認する手段とを有し、正当な権利をもち、かつ、操作権をもっているユーザからのデータのみを、制御系用リアルタイムオペレーティングシステム上で動作するプロセスにプロセス間通信し、制御系用リアルタイムオペレーティングシステム上では、さらに、制御コマンドを実行することが許可されている操作権であるかを確認する手段を有していることを特徴とする制御系用ファイアウォール。

【請求項5】請求項1記載の制御系用ファイアウォールであって、制御系用リアルタイムオペレーティングシ

テム上では、制御コマンドを前記監視制御用コンピュータに通信したとき、該監視制御用コンピュータより制御コマンドに対する進捗状況、または、結果を受信し、該進捗状況、または、結果を情報系オペレーティングシステム上で動作するプロセスにプロセス間通信する手段を有し、情報系オペレーティングシステム上では、プロセス間通信によって入手した進捗状況、または、結果を制御コマンドの発信元に転送する手段とを有していることを特徴とする制御系用ファイアウォール。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、不特定多数の人が利用する情報系ネットワークを利用して、プラントの監視制御を行うシステムにおいて、情報系ネットワークと制御系ネットワークとを安全に接続する装置に関する。

【0002】

【従来の技術】従来、例えば、下水処理場や排水機場などのプラントの監視制御は、専用のリアルタイムオペレーティングシステム（以下、RTOSという）で動作する制御機器・計測機器・制御装置・監視制御卓などを専用の回線で接続して制御系ネットワークを構築し、専用の制御系用通信プロトコルによって制御データ・監視データなどを通信する送ることによって行われてきた。

【0003】これに対し、企業をはじめとする様々な組織では、事務管理や電子メール・プリンタの共有などを目的として、組織内情報系ネットワーク（以下、イントラネットという）を構築している。一般に、情報端末には汎用のオペレーティングシステム（以下、GOSという）で動作するものを利用し、また、汎用の情報通信用プロトコルによって情報通信を行っている。さらに、イントラネットをインターネットに接続して、組織を超えたWWW（World Wide Web）サービスや電子メールも行っている。

【0004】インターネットを経由して、イントラネットに不正な侵入を防ぐものとしてファイアウォールがある。例えば、文献1（「ファイアウォール」、51頁～79頁、1995、ソフトバンク）によれば、ファイアウォールには、方式として、パケットフィルタリングゲートウェイ、トランスポートレベルゲートウェイ、アプリケーションレベルゲートウェイがある。

【0005】パケットフィルタリングゲートウェイは、送信元/送信先のIP（Internet Protocol）アドレス/ポートに基づいてパケットを遮断/許可する。トランスポートレベルゲートウェイは、送信元がトランスポートレベルゲートウェイのTCP（Transmission Control Protocol）ポートに接続すると、トランスポートレベルゲートウェイが別のネットワーク上のサーバのポートに接続する。コネクションが確立している間は、トランスポートレベルゲートウェイがリレーして、すべてのデータが

10

20

30

40

50

双方向に送られる。アプリケーションレベルゲートウェイは、送信元が別のネットワーク上のサーバのポートに接続要求をしたとき、アプリケーションレベルゲートウェイのTCPポートに接続し、アプリケーションレベルゲートウェイが要求のあったサーバのポートに接続要求する。

【0006】こうした状況において、制御系ネットワークとイントラネットとを接続し、情報系ネットワーク上の情報端末（イントラネット内の情報端末、インターネットを介して接続する情報端末、公衆回線・無線などを

使ってイントラネットに接続した情報端末など）からプラントの監視・制御、または、プラントの監視データの2次利用を行うシステムが要求されている。

【0007】上記のシステムを構築するためには、

（1）従来の制御系ネットワーク、および、制御用通信プロトコルを、情報系ネットワーク、および、情報系通信プロトコルに置き換えて再構築する方法と、（2）従来の制御系ネットワーク、および、制御用通信プロトコルを使って独自のイントラネットを構築し、その上に情報端末を接続する方法と、（3）従来の制御系ネットワーク、とイントラネットとを接続する方法とがある。このうち、（1）（2）は既に稼動しているプラント監視制御系、または、イントラネットを再構築する必要が生じ、それぞれに必要なサービスを業務に支障をきたさないように維持するのは大変である。また、いずれかが新規の構築になる場合であっても、それぞれに必要なサービスが一樣に同一のネットワーク上にあることは、制御系の役割を考えると、セキュリティやリアルタイム性の点で不安である。そこで、図2に示すように、制御系ネットワーク1000と情報系ネットワーク2000とを

分けて考え、それらを接続する。このとき、制御系のセキュリティやリアルタイム性を確保するために、制御系ネットワーク1000と情報系ネットワーク2000との接点に、制御系用ファイアウォール1が必要となる。

【0008】制御系用ファイアウォール1には、制御系ネットワークに接続するための制御系LANボード、および、情報系ネットワークに接続するための情報系LANボードを搭載し、制御系用通信プロトコルと、情報系用通信プロトコルとがサポートされている必要がある。両通信プロトコルをサポートするためには、RTOSに両通信プロトコルをサポートさせる方法と、GOSとRTOSの両方を共存させる方法が考えられる。

【0009】GOSとRTOSの両方を共存させる方法としては、例えば、文献2（「リアルタイム制御方式」、特開平10-21094）によれば、GOSが動作するCPUと、RTOSが動作するCPUとを搭載し、共有メモリを介して相互のプロセスの間のデータ交換を行う方法と、RTOSをコアにして、この上にGOSエミュレータを実装する方法とが紹介されている。

【0010】

【発明が解決しようとする課題】本発明の課題は、プラントの監視制御を行う制御系ネットワークと組織内情報系ネットワーク（イントラネット）を接続し、イントラネット上の情報端末などで、プラントデータの監視、または、プラントの制御を行うとき、制御系ネットワークのセキュリティ、および、リアルタイム性を確保するために、制御系ネットワークとイントラネットの接点に設置する制御系用ファイアウォールを提供することにある。

【0011】本発明の第1の課題は、制御系にとって有用なコマンドのみを制御系に転送するコマンドフィルタリング機能を有する制御系用ファイアウォールを提供することにある。

【0012】本発明の第2の課題は、制御系の状況に応じて有用なコマンドの制限を変更するアクティブコマンドフィルタリング機能を有する制御系用ファイアウォールを提供することにある。

【0013】本発明の第3の課題は、コマンドフィルタリングのルールを情報系ネットワーク上のいかなるプロセスからも覗くことができないようにするフィルタリングテーブル不可視化機能を有する制御系用ファイアウォールを提供することにある。

【0014】本発明の第4の課題は、権利のないユーザが制御できないように、かつ、権利をもつユーザでも他の権利者が制御を実行している間は制御できないようにするユーザ認証・操作権認証機能を有する制御系用ファイアウォールを提供することにある。

【0015】本発明の第5の課題は、制御コマンドを送信したとき、そのコマンドに対する制御系の進捗状況、または、結果をレポートするトランザクションモニタリング機能を有する制御系用ファイアウォールを提供することにある。

【0016】本発明の第6の課題は、不特定多数のユーザがプラントデータの監視ができ、かつ、不特定多数のリクエストが制御系にじょう乱を与えないようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【0017】本発明の第7の課題は、プラント監視データのヒストリカルデータも不特定多数のユーザが利用できるようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【0018】本発明の第8の課題は、プラント監視データをリアルタイムに必要とするユーザに対して、ユーザが毎回リクエストを要求しなくてもデータが配信され、かつ、要求のないプラント監視データはデータが配信されないようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【0019】本発明の第9の課題は、故障などのイベントが発生したときに、不特定多数のユーザに対してリアルタイムに配信され、かつ、後でイベント発生リストを

確認することもできるようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【0020】本発明の第10の課題は、RT-OSとG-OSとの双方に対して、メモリや記憶装置、LANボードなどに対して、アクセス領域が異なる制御系用ファイアウォールを提供することにある。

【0021】本発明の第11の課題は、制御系用ファイアウォール上に対するアクセスによって発生した事象を、不正・正当を問わずログをとる機能と、そのログを分析して適当な警報システムに状況報告をする機能を有する制御系用ファイアウォールを提供することにある。

【0022】

【課題を解決するための手段】(1) 制御系用ファイアウォールをG-OSとRT-OSが共存するコンピュータに実装する。G-OSとRT-OS上のそれぞれのプロセスは共有メモリを介してプロセス間通信ができるようにする。このとき、G-OS上の情報系プロセスで、暗号化データを受信し、そのデータを復号化し、復号化したデータをRT-OS上の制御系プロセスに渡す。この制御系プロセスで、データから制御コマンドを抽出し、コマンドフィルタリングテーブルを参照して、「通過」できるコマンドだけを制御系LAN上の監視制御コンピュータなどに転送する。

【0023】(2) 監視制御コンピュータなどからの監視データに基づいて、コマンドフィルタリングテーブルのルールを変更するロジックをもつプロセスをRT-OS上で実行させるか、または、監視制御コンピュータなどから直接ルールの変更要求を受け取れるようにする。

【0024】(3) コマンドフィルタリングテーブルをG-OS上の情報系プロセスからはアクセスできないメモリや記憶装置におく。

【0025】(4) 情報系プロセスにおいて、正当なユーザからのアクセスであるかを認証し、正当なユーザからのアクセスの場合、正当なユーザが利用している端末と制御系用ファイアウォールとの間でユニークな操作権番号を共有する。正当なユーザからの暗号化データを受信するが、それには、「ユーザID」「操作権番号」「制御コマンド」が含まれるようにする。そして、ユーザIDと操作権番号が一致するかをチェックする。もし、一致するならば、「操作権番号」と「制御コマンド」を制御系プロセスに転送する。制御系プロセスでは、「操作権番号」と「制御コマンド」を含むデータを受信し、操作権認証を行う。操作権認証は、受信した「操作権番号」と「制御コマンド」の組み合わせが一致するかを比較する。

【0026】(5) 制御系プロセスで、正当な制御コマンドを監視制御コンピュータなどに転送した後、制御コマンドを送出したことをプロセス間通信によって、情報系プロセスに通知し、情報系プロセスは、通知を受け取

ると、さらに、制御コマンドを発信したユーザ宛てに転送する。このサイクルを監視制御コンピュータなどから制御トランザクションに関するレポートが通知されるたびに繰り返す。

【0027】(6) 制御系プロセスで監視データを受信したとき、プロセス間通信で情報系プロセスに監視データを引き渡し、さらに、情報系プロセスは、情報系LAN上の端末やデータベースサーバに監視データを転送する。

【0028】(7) 情報系プロセスにおいて、タイマーを設定し、前回、データを転送したときの転送時刻よりも新しい時刻のものに更新されているものだけを取り出し、データベースサーバへまとめて転送する。そして転送時刻を更新する。

【0029】(8) 情報系プロセスにおいて、ユーザから、ある監視項目のリアルタイム配信要求を受けたとき、正当なユーザからの要求であるかを認証を行う。正当なユーザである場合には、その監視項目と配信先を登録する。この登録が済むと、指定されている監視項目の更新がある度に、登録されている配信先へ監視データを転送する。

【0030】(9) 情報系プロセスにおいて、イベント発生を受信する度に、イベント内容を情報系LAN上にマルチキャストする。

【0031】(10) 共有メモリに、G-OSから書き込み可能だが、RT-OSからは読み込みしかできないアドレス空間と、RT-OSから書き込み可能だが、G-OSからは読み込みしかできないアドレス空間を持たせる。

【0032】また、G-OSからしかアクセスできないメモリや記憶装置、LANボード、及び、RT-OSからしかアクセスできないメモリや記憶装置、LANボードを持たせる。

【0033】(11) 情報系プロセスにおいて、受信したデータを復号化したとき、送信元、ユーザ名、アクセス時刻、内容、処理状況のログをとる。定期、または、不定期に、このアクセスログを分析し、分析によってアクセス状況を認識し、重大、または、注意に値する状況になっている場合には、警報システムへ状況を報告する。

【0034】

【発明の実施の形態】図2は、制御系用ファイアウォールを介して情報系ネットワークと制御系ネットワークを接続するシステム構成例を示したものである。

【0035】制御系用ファイアウォール(ブランドファイアウォール)1は、制御系ネットワーク(制御系LAN)1000と、情報系ネットワーク(イントラネット)2000との間に接続される。制御系LAN1000には、監視制御コンピュータ1001が接続され、監視制御コンピュータ1001は、制御機器1002の制

御を行ったり、計測機器1003の計測データを取り込んだりしている。監視制御卓1004は制御コマンドの送信やデータの監視を行う。イントラネット2000には、情報サーバ2003、データベースサーバ2004、情報端末3001などが接続され、さらに、ファイアウォール2002を介してインターネット2001に接続している。情報端末3001としては、イントラネット2000上の他にも、公衆回線や無線回線など3002を介して情報サーバ2003の1つに接続するもの、インターネットサービスプロバイダ3003を介してインターネットに接続しているもの、他のネット上からインターネットに接続しているものなどがある。

【0036】図1、3、4、5は、制御系用ファイアウォールの第1の発明であるコマンドフィルタリング機能の実施例を示したものである。

【0037】制御系用ファイアウォール1は、制御系LANに接続する制御系LANボード14と、イントラネットに接続する情報系LANボード11とを搭載し、RTOS3とGOS2とが動作し、それぞれのOS上で、制御系用通信プロトコルによる通信9、情報系用通信プロトコルによる通信4で通信する機能を持っている。さらに、RTOS上のプロセス30とGOS上のプロセス20は、制御系-情報系間プロセス通信機能6、7によって共有メモリ10を介してプロセス間通信することができる。なお、図3以降の発明に関する図においては、通信プロトコル4、9、プロセス間通信6、7、メモリ・記憶装置など管理5、8に該当するものは割愛する。

【0038】情報系プロセス20では、暗号化データを受信し(21)、復号鍵を使って暗号化データを復号化する(22)。正当なデータならば、復号化データには制御コマンドが含まれている。そして、復号化データの一部、または、全部(制御コマンドを含む)を制御系-情報系間プロセス通信を使って制御系プロセス30に渡す(23)。制御系プロセス30で復号化データの一部、または、全部を受信し(31)、復号化データの中から制御コマンドをとりだし、その制御コマンドの通過・待機・遮断を行うコマンドフィルタリングを行い(32)、通過させる制御コマンド(正当なコマンド)のみを制御系LAN上の監視制御用コンピュータ1001などに転送する。

【0039】図3は、コマンドフィルタリングを行うためのフィルタリングテーブル34の例を示したものである。

【0040】フィルタリングテーブル34には、フィルタリング動作41、制御コマンド42、制御コマンドの送信先43が記述されており、RTOS3上のプロセス上から読み書き可能なメモリ、または、ハードディスクなどの記憶装置13に記憶されている。動作には、「通過」「待機」「遮断」がある。

【0041】図4、5は、コマンドフィルタリング32の具体的処理を示したものである。

【0042】受信した復号化データから抽出した制御コマンドがフィルタリングテーブル34に存在しているかを確認し(51)、コマンドが存在していない場合は、削除して(54)、終了する。存在する場合は、フィルタリング動作をチェックする(52)。動作が「遮断」のコマンドは、削除して(54)、終了する。「通過」のコマンドは、監視制御コンピュータなど指定されている送信先に送信する(33)。「待機」のコマンドは、コマンドの内容を保持し、別プロセスなどからの通知を待つ(53)。もし、別プロセスから通知があり、動作が「待機」から「通過」または「遮断」に変更になったときは、フィルタリング動作の再チェックを行う(52)。

【0043】しかし、もし、あるコマンドが連続して送信されたとき(制御トランザクションが完了しないうちに次のコマンドが送信されたとき)に、図4の処理だけでは不足である。そこで、図5に示したように、「通過」のコマンドに対しては、まず、そのフィルタリングルールの動作を一時「待機」にしておき(55)、コマンドを転送した(33)後、制御トランザクションの完了を待って(56)、完了を知った時点で、また、「通過」に戻す(57)。連続して送信されたコマンドは「待機」に基づき保持される。

【0044】以上によって、情報系LAN上の情報端末から行える制御を限定できる。不必要な制御コマンドがいたずらに制御系LAN上に流れることもない。制御トランザクションが完了しないうちに到着した制御コマンドにも対処できる。もし、一切の制御コマンドを排除したい場合には、フィルタリングテーブルの中味を無にすれば良い(記述のない制御コマンドは「遮断」を意味する)。

【0045】図6は、制御系用ファイアウォールの第2の発明であるアクティブコマンドフィルタリング機能の実施例を示したものである。

【0046】制御系プロセス60で、監視データ、または、フィルタリング動作変更要求を取得する(61)。フィルタリング動作変更要求(コマンドAを「通過」など)を取得した場合には、その通りにフィルタリングテーブルの変更を行う(63)。制御系プロセス60からアクセス可能なメモリまたは記憶装置13上に、フィルタリング動作を変更するためのルール65が存在する場合には、これに従って、入手した監視データを元に、動作変更の必要性があるかを調べ(62)、必要がある場合には、フィルタリングテーブルの変更を行う(63)。変更を行ったときは、別の制御系プロセスにもその旨を通知する(64)。フィルタリング動作を変更するためのルール65とは、例えば、「主電源がOFF状態のとき、緊急ポンプ停止の制御コマンドは遮断」など

のルールである。

【0047】監視制御コンピュータ1001側が、有効な制御コマンドを管理する機能を既にもっている場合（つまり、制御プロセス60の中の、動作変更要求の必要性の判断を行うロジック62相当のものを既に監視制御コンピュータが持っている場合）は、制御コマンドの有効／無効が切り替わったときのみ、その旨を制御系用ファイアウォール1に送信し、そのコマンドに対する動作の通過／遮断を切り替えることができる。監視制御コンピュータ1001側が、有効な制御コマンドを管理する機能を持っていない場合には、2つの方法がある。

(1) 監視制御コンピュータにロジックを実装する。

(2) 制御系用ファイアウォール1の制御系プロセス60に実装する。(2)の場合、例えば、制御系LAN上にたくさんの監視制御コンピュータがある場合でも、ロジックのメンテナンスを1箇所で行うことができる。逆に、ロジックが複雑、または、ルールを処理する数が多いと、制御系用ファイアウォール自身の負荷が大きくなる。

【0048】以上によって、例えば、ポンプ運転の状態に入ったら、保守コマンド系は遮断するとか、電源がONの状態でないとか、ポンプ運転系のコマンドは受け付けないなど、制御系の状態に基づく制御コマンドのフィルタリングができる。つまり、制御系の現在状態にとって不必要な制御コマンドがいたずらに制御系LAN上に流れることを防げる。

【0049】図7は、制御系用ファイアウォールの第3の発明であるフィルタリングテーブルの不可視化の実施例を示したものである。

【0050】G-OS2とRT-OS3が動作する制御系用ファイアウォールに対して、フィルタリングテーブルの記憶は、(a) 情報系プロセスからアクセス可能なメモリ、記憶装置12上、(b) 情報系プロセスからアクセス可能な共有メモリ10上、(c) 制御系プロセスからアクセス可能なメモリ、記憶装置13上の3つがある。

【0051】(a)の場合、情報系プロセス70aからアクセス可能なため、悪意のあるユーザによって例えばシステムのルート権限に不正侵入して、フィルタリングテーブル72aを書き換えてしまう可能性がある。フィルタリングテーブルが読み込みしかできないようになっている場合は、動的にフィルタリングテーブルを変更することができなくなる。また、読み込みができることを利用して、制御可能なコマンドをいたずらに送信してくる可能性もでてしまう。

【0052】(b)の場合も(a)と同様の問題がある。

【0053】これに対し、(c)の場合、情報系プロセス70cからは、直接的には、フィルタリングテーブルを参照することができないので、情報系LAN上の端末か

らは、制御可能なコマンド書き換えられることも、盗み見られることも可能性は極めて小さい。

【0054】第3の発明は、フィルタリングテーブル73を制御系プロセス71からのみアクセス可能なメモリ、記憶装置13上に記憶することで情報系プロセスから隠ぺいすることができる。

【0055】図8、9、10、11は、制御系用ファイアウォールの第4の発明であるユーザ認証・操作権認証機能の実施例を示したものである。

【0056】情報系プロセス80は、ユーザIDとパスワードとの組み合わせなどを用い、正当なユーザからのアクセスであるかを認証する(81)。そして、正当なユーザからのアクセスと判断されたときは、正当なユーザが利用している端末3001と制御系用ファイアウォール1との間でユニークな操作権番号84、85を共有する(82)。このとき、制御系用ファイアウォール1側ではユーザIDと操作権番号の組み合わせを暗号化して記憶しておくことが望ましい(83)。もし、同じユーザIDを使って別の端末からもアクセスがあるとしても、別の操作権番号が共有されることになる。

【0057】次に、情報系プロセス90は、正当なユーザからの暗号化データを受信し(21)、復号化する(22)。復号化したデータには、「ユーザID」「操作権番号」「制御コマンド」が含まれる。そして、ユーザIDと操作権番号が一致するかをチェックする(91)。もし、一致するならば、「操作権番号」と「制御コマンド」を制御系プロセスに転送する(23)。

【0058】制御系プロセス100は、「操作権番号」と「制御コマンド」を含む復号化データを受信し(31)、操作権認証を行ってから(101)、コマンドフィルタリングを行う(32)。このとき、図11に示したようにフィルタリングテーブル34には、制御コマンド42に対する操作権番号104が記憶されている。図中「-」で示されているのは、その制御コマンドが現在どのユーザにも利用しようとしていないことを意味する。操作権認証101は、受信した「操作権番号」と「制御コマンド」の組み合わせが一致するかを比較する(102)。もし、一致するならば、コマンドフィルタリングを行う(32)。もし、フィルタリングテーブルに操作権番号が登録されていないとき(図中「-」のとき)は、受信した操作権番号を該当の制御コマンド、および、それに関連する制御コマンドに登録してから(103)、コマンドフィルタリングを行う(32)。一致しないときは終了する。

【0059】その他に、制御系プロセスには、制御系コマンドと操作権番号との関連付けを空きににする手順が必要である。これは、利用者が操作権を放棄したり、または、一定時間以上操作がない(操作権の放棄の忘れ)、または、ある利用者の操作権を強制的にはく奪する場合に実行される。

【0060】以上によって、制御系にコマンドを送り込むことができるのは、正当なユーザだけである。しかも、他の正当なユーザが制御コマンドを実施中は、例えば、自分が正当ユーザであっても、制御コマンドを送り込むことはできない。図12は、制御系用ファイアウォールの第5の発明であるトランザクションモニタリング機能の実施例を示したものである。

【0061】制御系プロセス110では、正当な制御コマンドを転送した後(33)、制御コマンドを送出したことをプロセス間通信によって、情報系プロセス120に通知する(111)。情報系プロセスでは、通知を受け取ると、その内容を、さらに、制御コマンドを発信したユーザ宛てに転送する(122)。このサイクルを監視制御コンピュータなどから制御トランザクションに関するレポートが通知されるたびに繰り返し(113、121)、制御トランザクションが完了するまで繰り返す(112、123)。

【0062】以上によって、ユーザが送信した制御コマンドが正確に監視制御コンピュータ1001などに伝わったかを把握することができる。また、1つの制御コマンドに対してその制御トランザクションが完了するのに時間がかかる場合でも途中の進捗状況を把握することができる。

【0063】図13、14は、制御系用ファイアウォールの第6の発明である監視データ転送機能の実施例を示したものである。

【0064】制御系プロセス130では、監視データを制御系LAN上の監視制御コンピュータなどから受信し(131)、監視データをプロセス間通信によって、情報系プロセスに渡す(132)。実際には、図14に示したように共有メモリ10上の監視データ空間134に書き込まれ、ここには最新データ、及び、その更新時刻などの可変データが入る。一方、共有メモリ10上には、監視項目に対する属性情報空間133もあり、ここには、データID、データ名称、単位、共有メモリ上の監視データの保存アドレスなどが示される。属性情報空間133の内容は、監視項目の追加や削除・修正などがあった場合に制御系プロセス側から書き換えられるようになっている。

【0065】情報系プロセス140では、監視データを受信した後(141)、監視データを情報系LAN上の端末3001やデータベースサーバ2004などにさらに転送する(142)。また、必要に応じて、属性情報空間の内容を転送する場合もある。

【0066】以上によって、監視制御コンピュータ1001などがもつ制御機器や計測機器のデータを情報系上の端末やデータベースサーバに転送することができる。

【0067】上記の監視データの情報系LAN上の機器への転送の方法には、さらに、以下の3つの発明がある。

【0068】図15、16は、監視データの転送機能における大容量データ転送機能の発明(制御系用ファイアウォールの第7の発明)の実施例を示したものである。

【0069】まず、タイマーイベントが発生する初期時刻、及び、時間間隔159をセットしておく(151)。

【0070】情報系プロセス150では、タイマーイベントが発生すると(152)、前回、データをデータベースサーバ2004へ転送したときの転送時刻158を読み込む(153)。監視データを受信し(共有メモリ10上のデータを読み込み)(141)、前回転送時刻よりも新しい時刻のデータであるかをチェックする(154)。データが新しいときは、そのデータを一時記憶する(155)。これをすべての監視データに対して繰り返す(156)。そして、一時記憶しておいた監視データをデータベースサーバ2004へまとめて転送する(142)。転送した監視データの中で最も新しい更新時刻を最終転送時刻158として書き換える(157)。

【0071】上記を図16の具体的な例で説明する。この例では、12:00を基点として、20分ごとにタイマーイベントが発生するように設定されており、現在時刻は、13:20になった場合である。前回の最終転送時刻は13:00と記憶されており、監視データ空間134上のデータから13:00よりも新しいものを一時記憶空間164に抽出し、抽出したデータをまとめてデータベースサーバに転送する。そして、最終転送時刻を最も新しいものである13:15におきかえる。なお、この例において、最終転送時刻を現在時刻の13:20とする場合もある。

【0072】以上によって、データベースサーバ2004に定期的にデータを一括して転送することができる。監視データ空間のデータの更新時刻が同一でなくても問題ない。このとき、更新されていないデータに関しては、転送されないで、トラフィックの節約にもなるし、一度送ったことのあるデータの再送によるデータベースサーバ側の負荷低減にもなる。また、通常、制御系上での監視データの更新サイクルはかなり短く、このサイクルに合わせて全てのデータを転送するのは、相当負荷が大きい。時間間隔の設定ができるので、転送サイクルを長くすることで、制御系プラントファイアウォール・ネットワークトラフィック・データベースサーバの負荷を抑えることができる。

【0073】図17は、監視データの転送機能におけるリアルタイム配信機能の発明(制御系用ファイアウォールの第8の発明)の実施例を示したものである。

【0074】情報系プロセス160では、ある監視項目のリアルタイム配信要求を受信すると(161)、まず、そのユーザの認証を行う(81)。正当なユーザである場合には、その監視項目と配信先を登録する(16

2)。

【0075】上記の登録があると、情報系プロセス140では、指定されている監視項目の更新がある度に(141)、登録されている配信先へ転送する(142)。

なお、配信先は1箇所でない場合もある。

【0076】以上によって、情報系LAN上の端末は、リアルタイム配信を受けることができる。また、ユーザ認証を加えていることにより、なりすましによってリアルタイム配信サービスの妨害することから防ぐこともでき

る。なお、リアルタイム配信は、1ユーザあたり3項目までのように制約をつけてリアルタイム配信サービスを保護してもよい。

【0077】図18は、監視データの転送機能におけるイベントのマルチキャスト配信機能の発明(制御系用ファイアウォールの第9の発明)の実施例を示したものである。

【0078】情報系プロセス170では、イベント発生を受信する度に(171)、イベント内容を情報系LAN上にマルチキャストする(172)。情報系LAN上のデータベースサーバ2004、端末3001はマルチキャストを受信すると、イベント内容を取り込み、データベースサーバにイベントを取り込んだり、端末にイベントを表示したりなどの適切な処置を行う。

【0079】以上によって、マルチキャストを受信する体制になっている情報系LAN上の端末、データベースサーバは、イベントをリアルタイムに受信することができる。また、端末が受信する体制になかったとしても、データベースサーバには、発生イベントが格納されているので、こちらを参照することでイベントリストを見る

ことができる。

【0080】図19は、制御系用ファイアウォールの第10の発明であるメモリアクセスの安全性の実施例を示したものである。

【0081】制御系用ファイアウォール1は、G-OS2とRT-OS3が実装され、それぞれ共有メモリ10にアクセスすることができる。このとき、共有メモリは、G-OS2から書き込み可能だが、RT-OS3からは読み込みしかできないアドレス空間181と、RT-OS3から書き込み可能だが、G-OS2からは読み込みしかできないアドレス空間182とを持たせる。アドレス空間181には、例えば、制御コマンドや、適当な各種フラグが、G-OS側のプロセスによって書き込まれる。アドレス空間182には、例えば、属性情報や、適当な各種フラグ、監視データ、イベント、制御トランザクションのレポートなどが、RT-OS側のプロセスによって書き込まれる。

【0082】以上によって、G-OS上のプロセスが誤って、監視データやイベントなどを書き換えてしまうことがなくなる。また、共有メモリを介したプロセス間通

信として、お互いに通信の受領を通知したい場合でも、両方の空間にそれぞれのOSのプロセスがフラグを書き込むための領域があるので、問題ない。

【0083】図20は、制御系用ファイアウォールの第11の発明であるメモリアクセスの安全性の第2の実施例を示したものである。

【0084】制御系用ファイアウォール1は、G-OS2とRT-OS3が実装され、それぞれ共有メモリ10にアクセスすることができるが、G-OS2からしかアクセスできないメモリや記憶装置12、LANボード11、及び、RT-OS3からしかアクセスできないメモリや記憶装置13、LANボード14を持たせる。例えば、G-OS2は、メモリ13を認識することはできない。

【0085】以上によって、例えば、コマンドフィルタリングテーブル34をメモリ13に置くことで、G-OS側のプロセスからは、その内容を直接読んだり、書き換えたりすることはできない。

【0086】図21は、制御系用ファイアウォールの第12の発明であるアクセスログ機能の実施例を示したものである。

【0087】情報系プロセス190では、暗号化してある、または、平文のままのデータを受信する(21)。そして、その内容を復号化する(22)。当然、平文は復号化処理を施せば意味のないものにかわる。そして、復号化したデータが、意味のあるものかどうかを判断し(191)、意味不明の場合には、内容が不正であるとして、処理を「不正による削除(192)」として、送信元、ユーザ名、アクセス時刻、内容、処理状況のログ195をとる(194)。復号化した内容に意味がある場合には、ユーザIDや操作権番号が一致するかを確認し(91)、不一致の場合には、「処理：操作権不一致による削除(193)」として、同様にログ195をとる(194)。一致の場合には、「処理：正当なデータ転送」として、内容をプロセス間通信によって、制御系プロセスに引き渡す。このときもログ195をとる(194)。

【0088】図22は、制御系用ファイアウォールの第13の発明である警報機能の実施例を示したものである。

【0089】情報系プロセス200では、定期、または、不定期に、アクセスログ195を分析する(201)。分析によってアクセス状況を認識し(202)、もし、重大、または、注意に値する状況になっている場合には、警報システムへ状況を報告する(203)。問題なければ、特に何もしない。

【0090】以上によって、正当、不正を含めてアクセスの状況が内容レベルまでログをとり、さらに、重大な不正があった場合には、即座に警報システムに報告がで

【0091】

【発明の効果】本発明によれば、情報系LAN上の情報端末3001から行える制御を限定できる。不必要な制御コマンドがいたずらに制御系LAN上に流れることもない。制御トランザクションが完了しないうちに到着した制御コマンドにも対処できる。もし、一切の制御コマンドを排除したい場合には、フィルタリングテーブルの中味を無にすれば良い。

【0092】本発明によれば、例えば、ポンプ運転の状態に入ったら、保守コマンド系は遮断するとか、電源がONの状態でないとか、ポンプ運転系のコマンドは受け付けないなど、制御系の状態に基づく制御コマンドのフィルタリングができる。つまり、制御系の現在状態によって不必要な制御コマンドがいたずらに制御系LAN上に流れることを防げる。

【0093】本発明によれば、フィルタリングテーブルを制御系プロセスからのみアクセス可能なメモリ、記憶装置上に記憶することで情報系プロセスから隠ぺいすることができる。

【0094】本発明によれば、制御系にコマンドを送り込むことができるのは、正当なユーザだけである。しかも、他の正当なユーザが制御コマンドを実施中は、例えば、自分が正当ユーザであっても、制御コマンドを送り込むことはできない。本発明によれば、ユーザが送信した制御コマンドが正確に監視制御コンピュータなどに伝わったのかを把握することができる。また、1つの制御コマンドに対してその制御トランザクションが完了するのに時間がかかる場合でも途中の進捗状況を把握することができる。

【0095】本発明によれば、監視制御コンピュータなどがもつ制御機器や計測機器のデータを情報系上の端末やデータベースサーバに転送することができる。

【0096】本発明によれば、データベースサーバに定期的にデータを一括して転送することができる。監視データ空間のデータの更新時刻が同一でなくても問題ない。このとき、更新されていないデータに関しては、転送されないで、トラフィックの節約にもなるし、一度送ったことのあるデータの再送によるデータベースサーバ側の負荷低減にもなる。また、通常、制御系上での監視データの更新サイクルはかなり短く、このサイクルに合わせて全てのデータを転送するのは、相当負荷が大きい。時間間隔の設定ができるので、転送サイクルを長くすることで、制御系プラントファイアウォール・ネットワークトラフィック・データベースサーバの負荷を抑えることができる。

【0097】本発明によれば、情報系LAN上の端末は、リアルタイム配信を受けることができる。また、ユーザ認証を加えていることにより、なりすましによってリアルタイム配信サービスを不正に大量に行って、リアルタイム配信サービスの妨害することから防ぐこともで

きる。

【0098】本発明によれば、マルチキャストを受信する体制になっている情報系LAN上の端末、データベースサーバは、イベントをリアルタイムに受信することができる。また、端末が受信する体制になかったとしても、データベースサーバには、発生イベントが格納されているので、こちらを参照することでイベントリストを見ることができる。

【0099】本発明によれば、G-OS上のプロセスが誤って、監視データやイベントなどを書き換えてしまうことがなくなる。また、共有メモリを介したプロセス間通信として、お互いに通信の受領を通知したい場合でも、両方の空間にそれぞれのOSのプロセスがフラグを書き込むための領域があるので、問題ない。

【0100】本発明によれば、例えば、コマンドフィルタリングテーブルをメモリに置くことで、G-OS側のプロセスからは、その内容を直接読んだり、書き換えたりすることはできない。

【0101】本発明によれば、正当、不正を含めてアクセスの状況が内容レベルまでログをとり、さらに、重大な不正があった場合には、即座に警報システムに報告がでる。

【図面の簡単な説明】

【図1】本発明のコマンドフィルタリング機能の実施例の説明図である。

【図2】制御系用ファイアウォールを含めた全体システムの例である。

【図3】本発明のコマンドフィルタリング機能の実施例の第1の説明図である。

【図4】本発明のコマンドフィルタリング機能の実施例の第2の説明図である。

【図5】本発明のコマンドフィルタリング機能の実施例の第3の説明図である。

【図6】本発明のアクティブコマンドフィルタリング機能の実施例の説明図である。

【図7】本発明のコマンドフィルタリングテーブルの不可視化の実施例の説明図である。

【図8】本発明のユーザ認証・操作権認証機能の実施例の第1の説明図である。

【図9】本発明のユーザ認証・操作権認証機能の実施例の第2の説明図である。

【図10】本発明のユーザ認証・操作権認証機能の実施例の第3の説明図である。

【図11】本発明のユーザ認証・操作権認証機能の実施例の第4の説明図である。

【図12】本発明の制御トランザクションのレポート機能の実施例の説明図である。

【図13】本発明の監視データの転送、及び、その拡張機能の実施例の第1の説明図である。

【図14】本発明の監視データの転送、及び、その拡張

機能の実施例の第2の説明図である。

【図15】本発明の監視データの転送、及び、その拡張機能の実施例の第3の説明図である。

【図16】本発明の監視データの転送、及び、その拡張機能の実施例の第4の説明図である。

【図17】本発明の監視データの転送、及び、その拡張機能の実施例の第5の説明図である。

【図18】本発明の監視データの転送、及び、その拡張機能の実施例の第6の説明図である。

【図19】本発明のメモリアクセスの安全性確保の実施例の第1の説明図である。

【図20】本発明のメモリアクセスの安全性確保の実施例の第2の説明図である。

【図21】本発明のアクセスログ、及び、警報機能の実

* 施例の第1の説明図である。

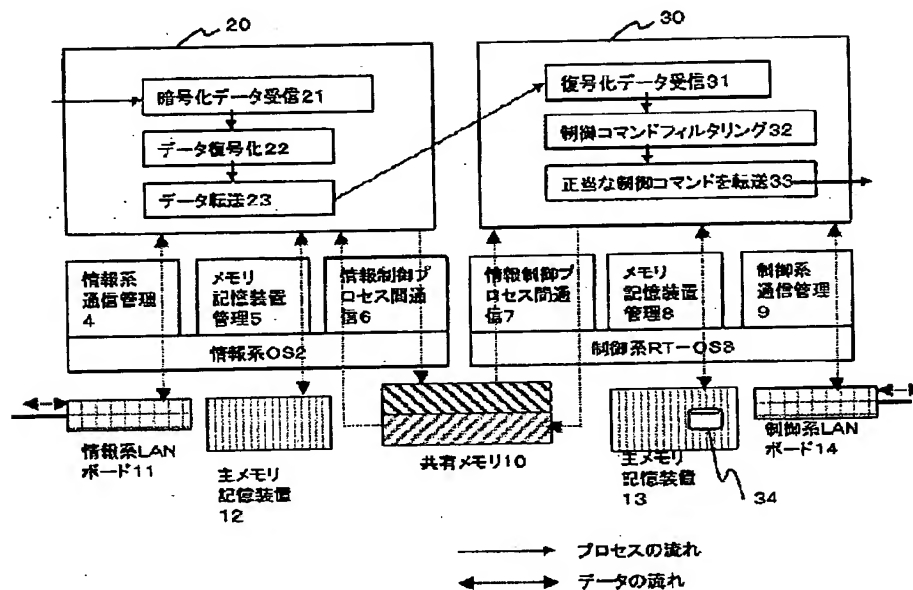
【図22】本発明のアクセスログ、及び、警報機能の実施例の第2の説明図である。

【符号の説明】

1…制御系用ファイウォール（プラントファイアウォール）、2…情報系OS（G-OS）、3…制御系RT-OS（RT-OS）、10…共有メモリ、11…情報系LANボード、12…情報系メモリ・記憶装置、13…制御系メモリ・記憶装置、14…制御系LANボード、34…コマンドフィルタリングテーブル、1000…制御系LAN、1001…監視制御コンピュータ、1002…制御機器、1003…計測機器、2000…情報系LAN（イントラネット）、2001…インターネット、2004…データベースサーバ、3001…情報端末。

【図1】

図1



【図3】

図3

動作41	制御コマンド42	送信先43
通過	カメラズーム	カメラ制御装置
遮断	カメラチルト	カメラ制御装置
待機	ポンプ起動	制御コンピュータA
待機	ポンプ停止	制御コンピュータA
遮断	ポンプ保守	制御コンピュータA
通過	ゲート開	制御コンピュータA
通過	ゲート閉	制御コンピュータA

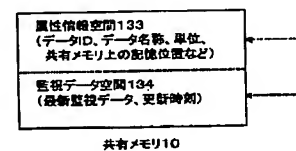
【図11】

図11

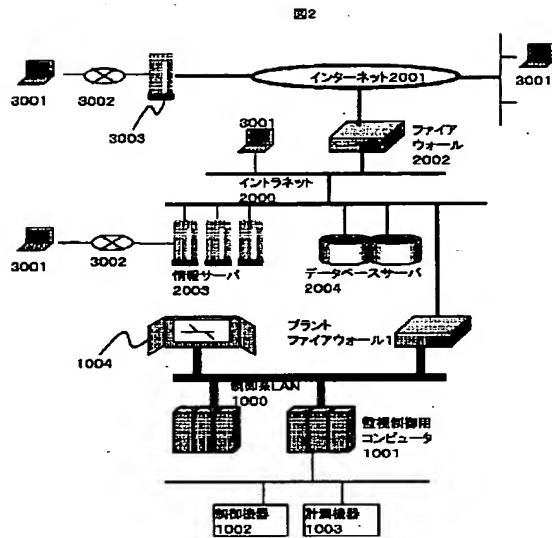
動作41	制御コマンド42	操作障害号104
通過	カメラズーム	R2913
遮断	カメラチルト	R2913
待機	ポンプ起動	—
待機	ポンプ停止	—
遮断	ポンプ保守	—
通過	ゲート開	R315
通過	ゲート閉	R315

【図14】

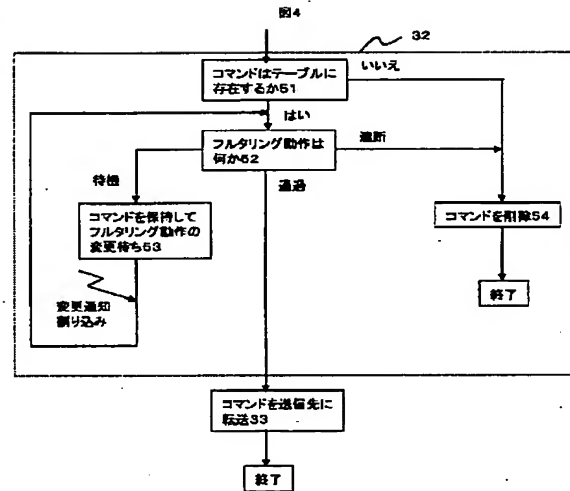
図14



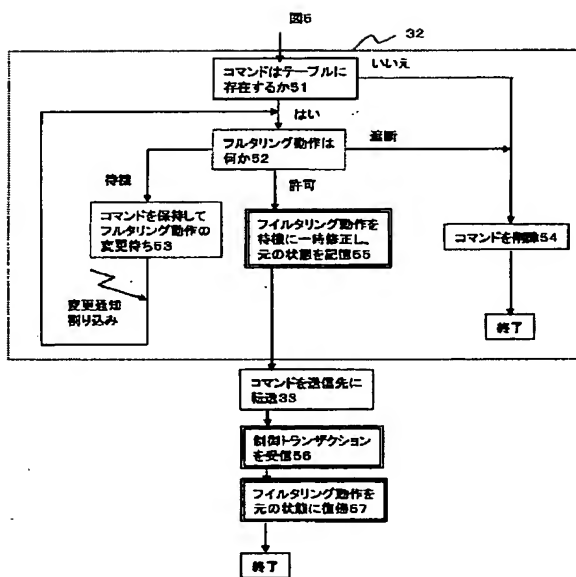
【図2】



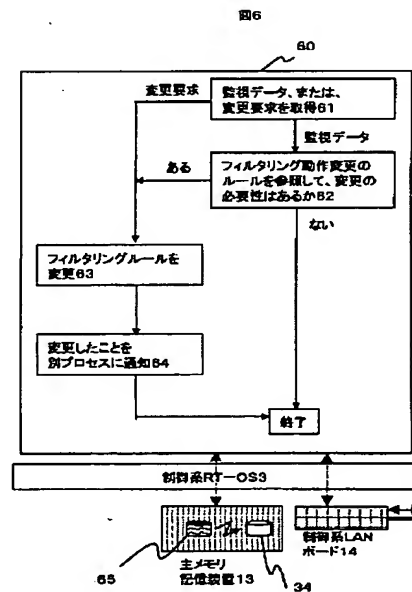
【図4】



【図5】

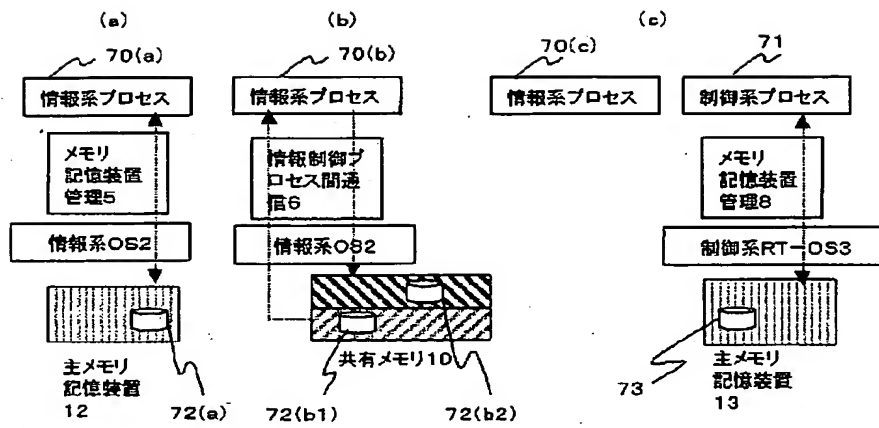


【図6】



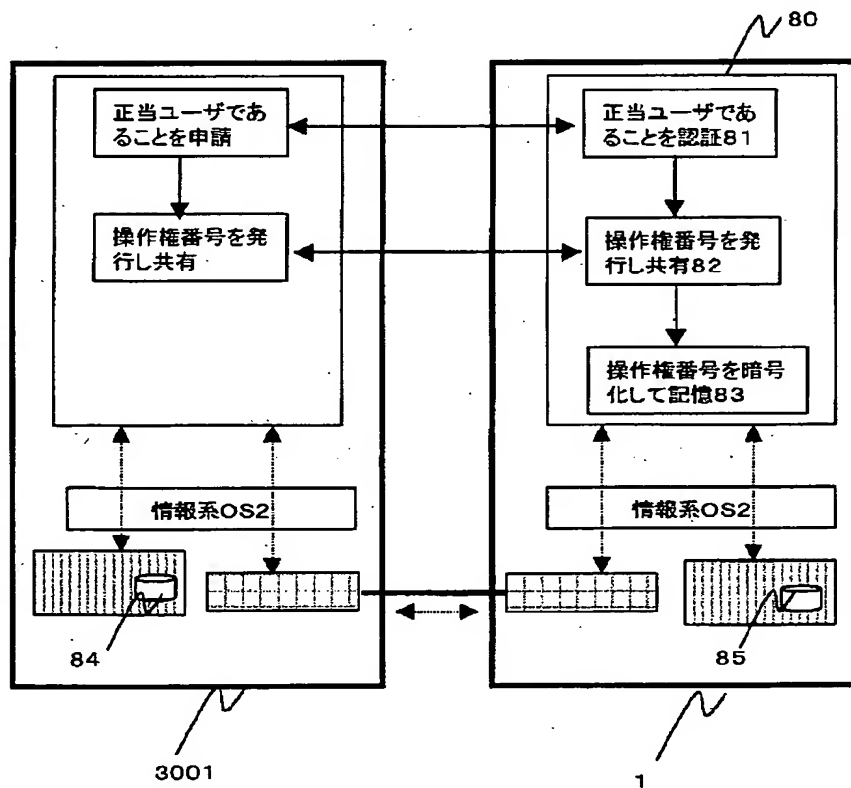
【図7】

図7



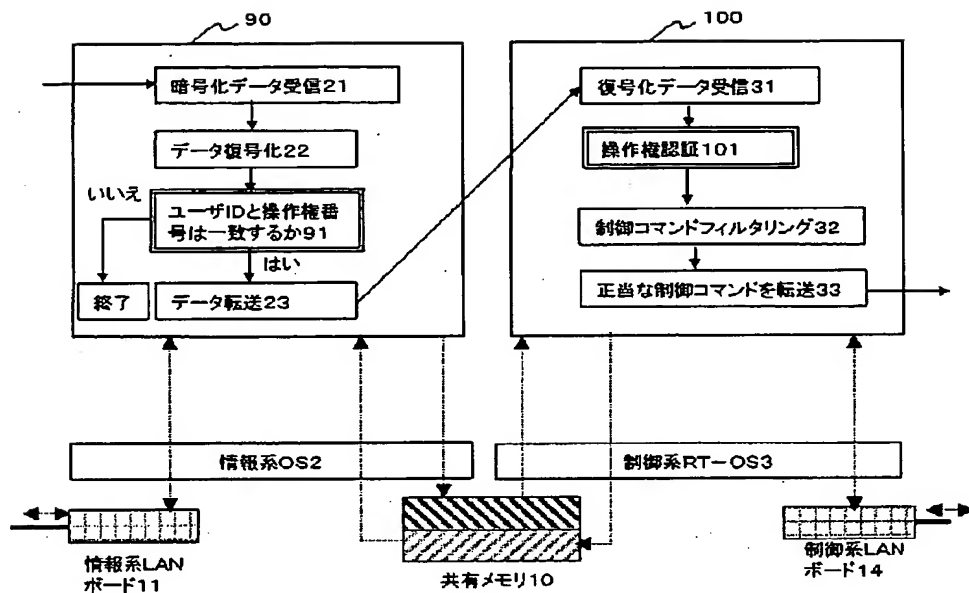
【図8】

図8



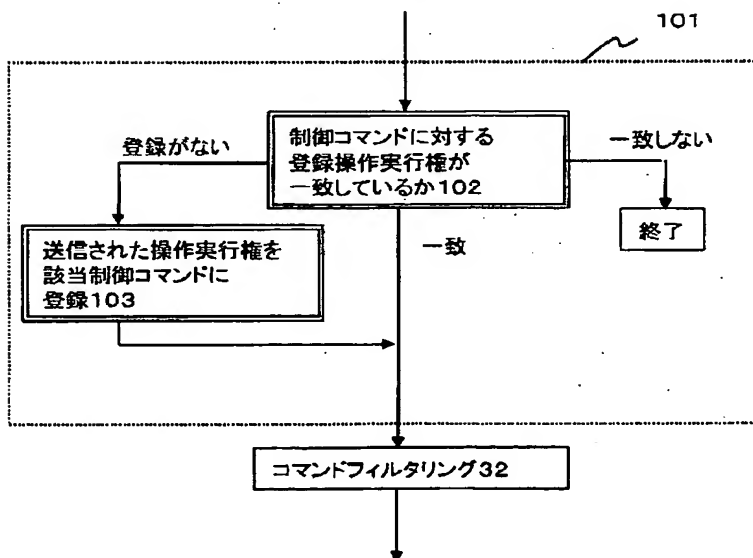
【図9】

図9



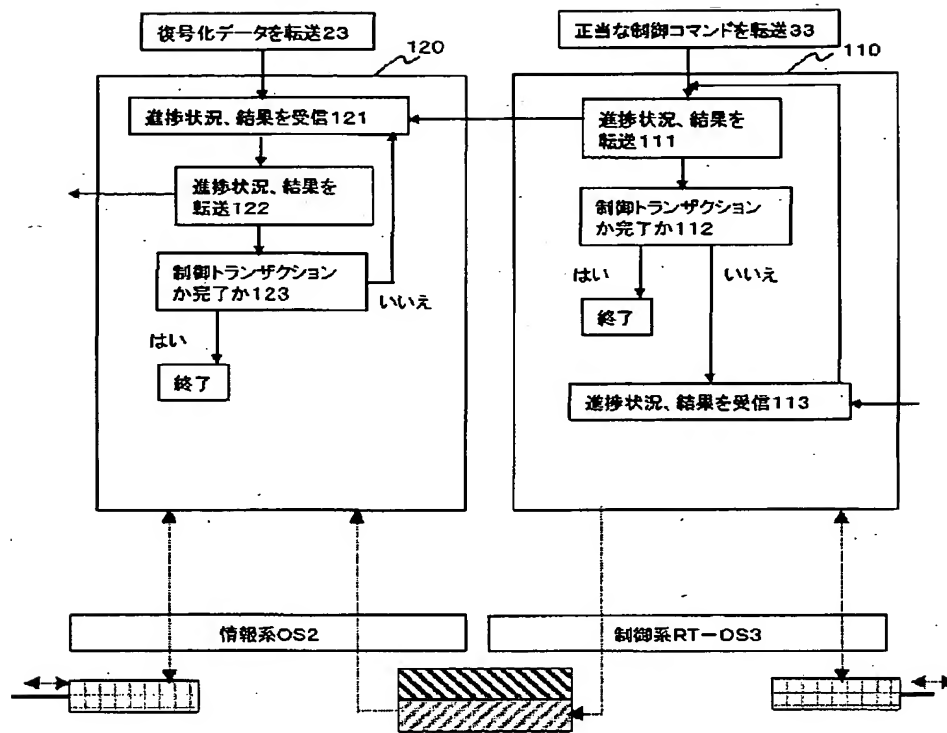
【図10】

図10



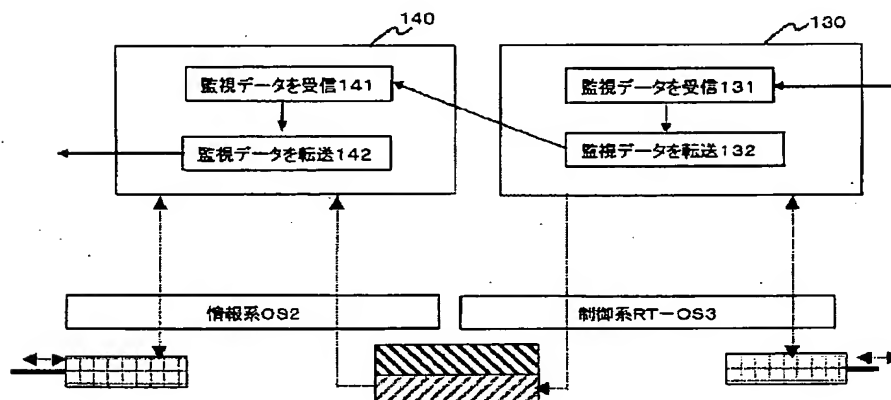
【図12】

図12



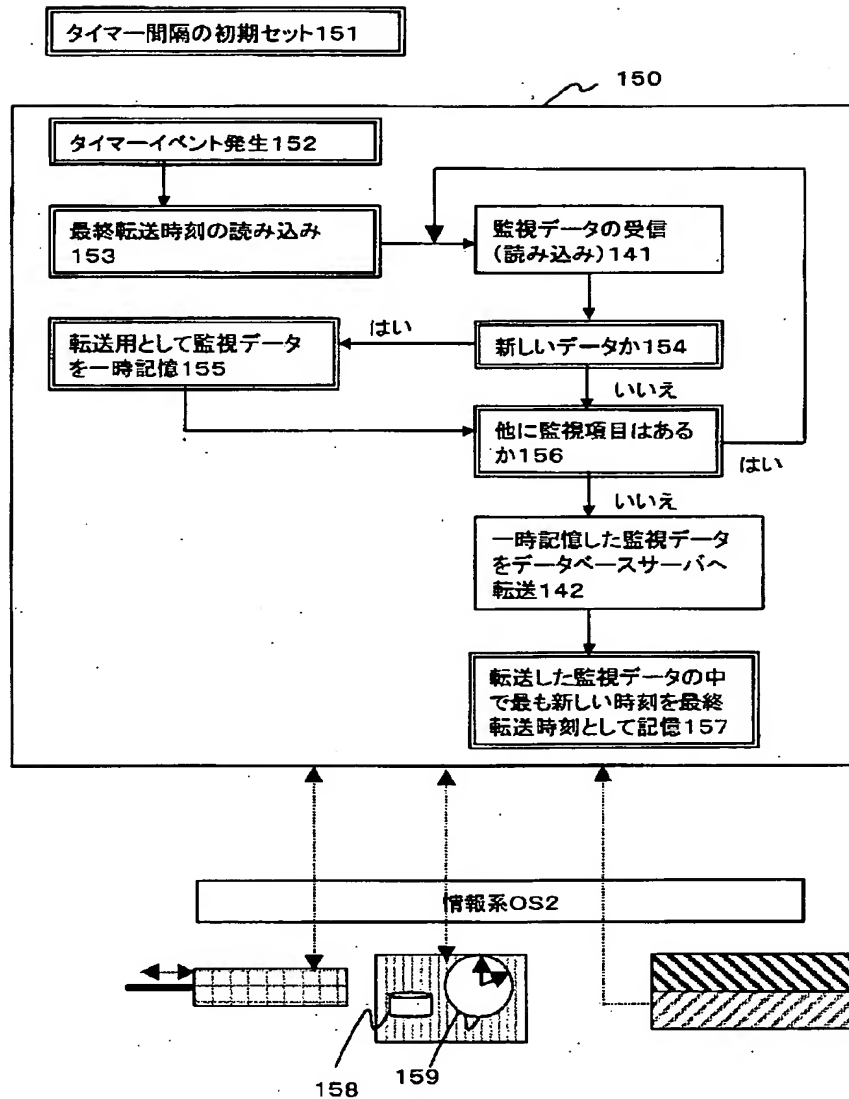
【図13】

図13



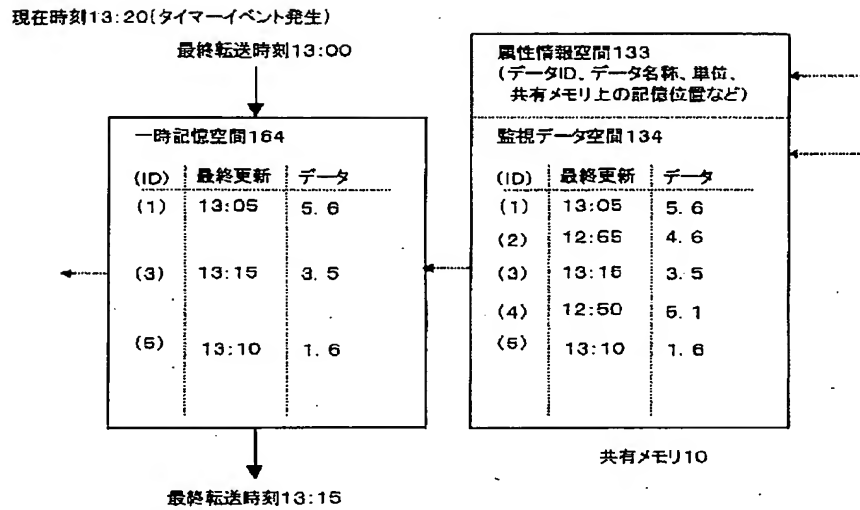
【図15】

図15



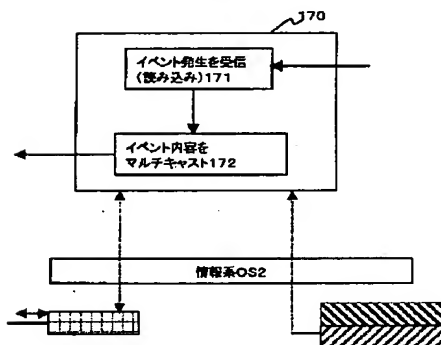
【図16】

図16



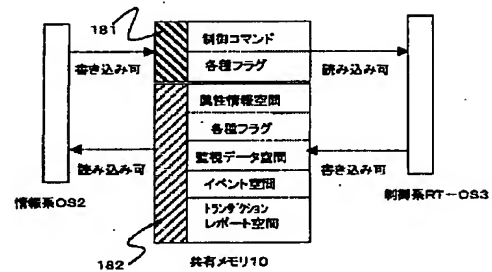
【図18】

図18



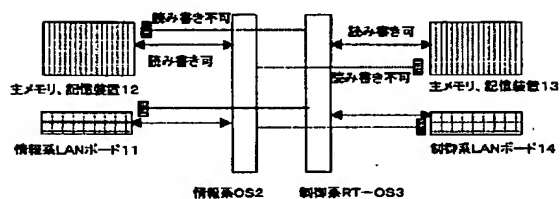
【図19】

図19

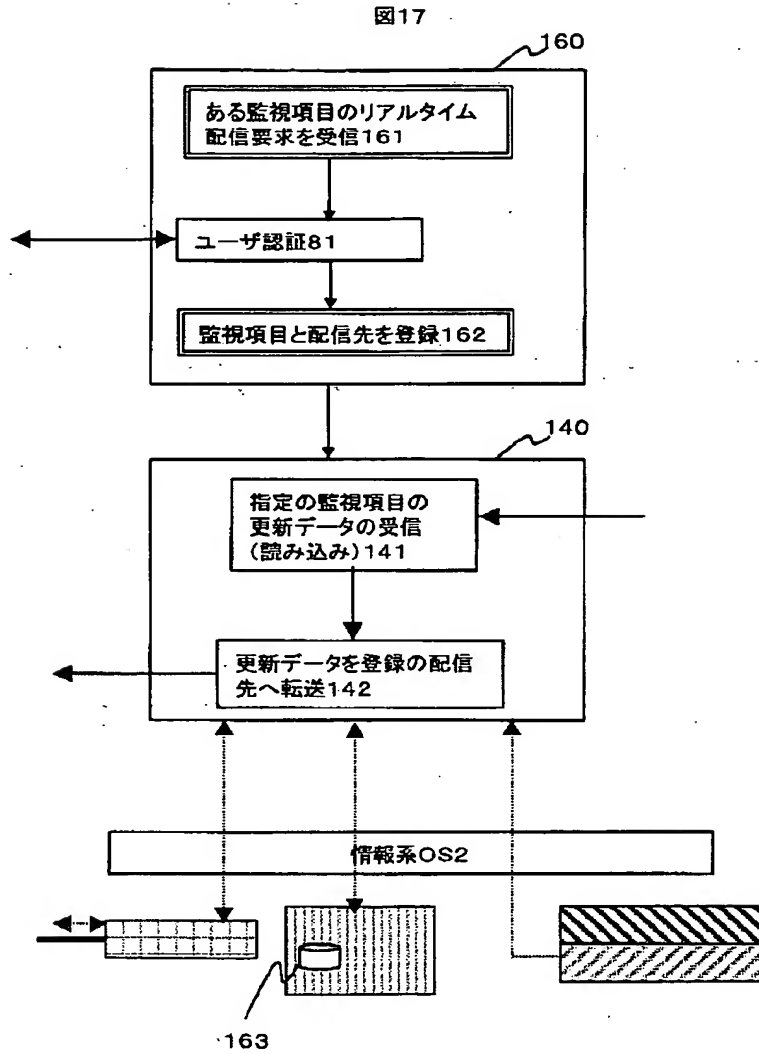


【図20】

図20

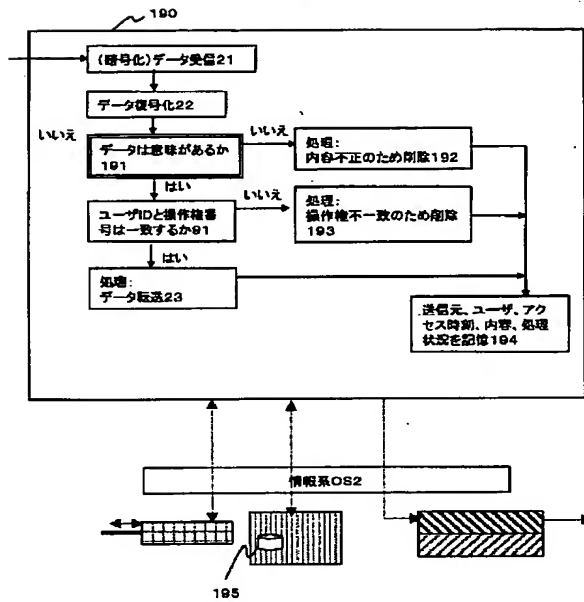


【図17】



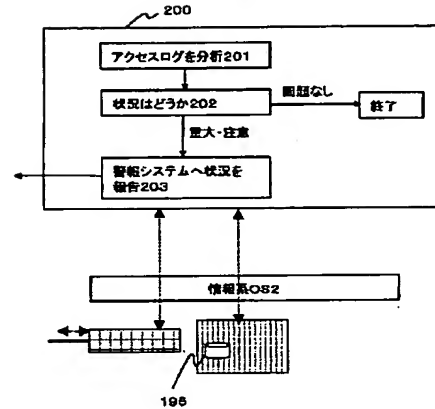
【図21】

図21



【図22】

図22



フロントページの続き

(72)発明者 加藤 博光
 神奈川県川崎市麻生区王禅寺1099番地 株
 式会社日立製作所システム開発研究所内

Fターム(参考) 5B089 GA01 GA11 HA06 HA10 JA35
 JB10 JB16 KA17 KB04 KB13
 KC32 KC53 KC58 KH01
 5B098 AA10 GA02 GA04 GC16
 5K033 AA08 CB01 CB08 DA01 DA05
 DB10 DB12 DB14 DB16 EA07